CUAUHTEMOC ORTEGA (Bar No. 257443)
Federal Public Defender
GEORGINA WAKEFIELD (Bar No. 282094)
(E-Mail: Georgina_Wakefield@fd.org)
GABRIELA RIVERA (Bar No. 283633)
(E-Mail: Gabriela_Rivera@fd.org)
JULIA DEIXLER (Bar No. 301954)
(E-Mail: Julia_Deixler@fd.org)
Deputy Federal Public Defenders
321 East 2nd Street
Los Angeles, California 90012-4202
Telephone: (213) 894-2854
Facsimile: (213) 894-0081

Attorneys for Defendant
JERRY NEHL BOYLAN

UNITED STATES DISTRICT COURT

CENTRAL DISTRICT OF CALIFORNIA

WESTERN DIVISION

UNITED STATES OF AMERICA, Plaintiff, v. JERRY NEHL BOYLAN, Defendant.	Case No. 2:22-CR-00482-GW **DEFENDANT JERRY NEHL BOYLAN'S REPLY TO GOVERNMENT'S OPPOSITION TO MOTION TO COMPEL GOVERNMENT TO PERMIT DEFENSE EXAMINATION OF DIGITAL DEVICES; EXCLUDING DATA FROM THE DEVICES AT TRIAL IN THE ALTERNATIVE**

Jerry Nehl Boylan, through his attorneys of record, Deputy Federal Public Defenders Georgina Wakefield, Gabriela Rivera, and Julia Deixler, files his reply to the government's opposition to motion to compel the government to permit a defense examination of the digital devices recovered from the wreckage of the Conception or to exclude any data from these devices at trial.

Respectfully submitted,

CUAUHTEMOC ORTEGA
Federal Public Defender

DATED: April 10, 2023

By */s/ Georgina Wakefield*
GEORGINA WAKEFIELD
Deputy Federal Public Defender

I. INTRODUCTION

The government's opposition rests on a legally incorrect premise: that a deceased has a Fourth Amendment right against unreasonable searches and seizures after death. The government contends that despite having in its possession decedents' digital devices and forensic copies of their entire contents, it does not possess them under Rule 16 because the Fourth Amendment prevents the government from accessing them. The government is wrong. Under well-settled precedent, the deceased do not possess Fourth Amendment privacy rights. Thus, while the government chose to obtain warrants and consent to search the devices, it was under no constitutional or legal obligation to do so. The same is still true—the Fourth Amendment does not prevent the government from accessing the data on the devices. As a result, the Fourth Amendment does not prevent the government from turning the devices over to the defense. Accordingly, the government's entire opposition rests on an incorrect legal premise and should be rejected.

In the end, the government's opposition asks the Court to blindly trust that its agent did a thorough job analyzing the devices despite: (a) incorrectly believing that a warrant or consent to search were constitutionally required; (b) misinterpreting "materiality" under Rule 16 as requiring that evidence be exculpatory; (c) taking a narrower view of the relevant timeframe than what is charged in the Indictment; and (d) declining to identify the search protocol the agent used to analyze the devices and seize minimal data.

II. ARGUMENT

A. Because the decedents do not have Fourth Amendment rights, the government can access the digital devices without a warrant or consent, and so the devices are in the government's possession.

A decedent does not have constitutional rights after death. *See Guyton v. Phillips*, 606 F.2d 248, 250 (9th Cir. 1979) ("A 'deceased' is not a 'person' for the

purposes of 42 U.S.C. §§ 1983 and 1985, nor for the constitutional rights which the Civil Rights Act serves to protect."); *Whitehurst v. Wright*, 592 F.2d 834, 840 (5th Cir. 1979) ("After death, one is no longer a person within our constitutional and statutory framework, and has no rights of which he may be deprived."). "Generally, the term 'person,' as used in a legal context, defines a living human being and excludes a corpse or human being who has died." *Guyton*, 606 F.2d at 250 (citations omitted). Because the Fourth Amendment grants privacy protections to "people," a decedent cannot invoke those protections. Banta, *Death and Privacy in the Digital Age*, 94 N.C. L. REV. 927, 939-40 (2016) (describing how decedents have no privacy protections under constitutional or statutory law).

Nor do a decedent's next of kin have Fourth Amendment rights that would prevent the government from accessing the data. "Fourth Amendment rights are personal rights which . . . may not be vicariously asserted." *Alderman v. United States*, 394 U.S. 165, 174 (1969). This issue commonly arises in the context of autopsies performed against the wishes of a decedent's survivors. Because Fourth Amendment rights cannot be vicariously asserted, courts hold that survivors have no Fourth Amendment rights with regard to an autopsy performed on the body of their deceased relative, including no privacy interest in the blood, tissue, or organs removed during an autopsy. *See*, *e.g.*, *Love v. Bolinger*, 927 F. Supp. 1131, 1136 (S.D. Ind. 1996); *Hubenscmidt v. Shears*, 270 N.W.2d 2 (Mich. 1978).

Despite these well-established constitutional principles, the government claims in its opposition that the decedents have "significant and Constitutionally protected privacy interests in the unseized data" that prevent the government from accessing the data on the devices. (Gov't Opp. at 8:1-2.) In fact, the government devotes 12 pages of its argument section to legal argument and citation that assumes that decedents and

their survivors have Fourth Amendment rights with respect to the devices.[1] The government cites no case holding that decedents or their next of kin have a constitutionally protected right or expectation of privacy in the data on the devices because no such case exists.

The lack of Fourth Amendment protections eviscerates the government's claim that it does not possess the devices or their data, which rests on this legally incorrect premise. Because no person has a legally cognizable expectation of privacy in the digital devices, the government did not and still need not obtain a search warrant or consent to search the devices or access the data. For that reason, the cases relied on by the government are distinguishable. The *Huizar*, *Collins*, and *Salyer* cases all involved third parties who were living and had an expectation of privacy in the data. (Gov't Opp. at 10-11.) The courts in those cases held that because a warrant was required, the government lacked authority to go back and search materials outside the scope of the original search warrant. Because no warrant is required here, those cases are not on point.

The government attempts to distinguish *Halgat* by repeating the same legally incorrect premise. It argues, "[t]he privacy interests underlying the Fourth Amendment and the government's limitations on accessing third-party devices [] were non-existent

---

[1] "[D]efendants cannot compel the government to violate other people's Fourth Amendment rights simply to satisfy a defendant's curiosity." (Gov't Opp. at 10:9-11.)

"But the only 'absurd result' here would be eviscerating the requirements of Rule 41 and the core tenets of the Fourth Amendment by giving defendants free reign over the entire of any third party's digital device simply to check the government's work." (Gov't Opp. at 12:5-8.)

"As in virtually all cases involving digital devices, the government was required to obtain court-authorized search warrants or limited contents here to search the victim-decedents' Subject Devices given the Fourth Amendment and the fundamental privacy interests at stake. Those Constitutional constraints and privacy interests are no less paramount now." (Gov't Opp. at 13:23-28.)

"The same privacy interests still apply to the next-of-kin of the victim who provided a limited consent to the government to search their deceased family member's digital device." (Gov't Opp. at 18-20.)

in *Halgat*." (Gov't Opp. at 16:13-17.) Again, there are no Fourth Amendment privacy interests in the devices here, so the government only proves the defense's point that *Halgat* is persuasive authority. Just as here, the agent in *Halgat* did not have an expectation of privacy in his government-issued phone and therefore the government had an obligation to turn the contents of the device over to the defense after it made out a low showing of materiality under Rule 16. The result here should be the same.

B. The defense has met the "low threshold" for materiality.

The Motion and accompanying *in camera* filing set forth several bases for the Court to find that a complete inspection of the seized digital devices is material under Rule 16. These broadly include: (1) additional evidence likely to be found on the devices that the government's case agent did not flag as relevant but that is material to preparing the defense, and (2) information that the defense may obtain from its own examination of the devices, which is both material to preparing the defense and is intended to be used by the government at trial.

As to the first category of information, the government takes an unjustifiably narrow view of materiality. The government misreads the caselaw in seemingly assuming that information is only "helpful to the defense" if it is exonerating or exculpatory. (Gov't Opp. at 4 n.2) ("Given the incriminating nature of the evidence recovered from the other three digital devices . . . it is highly unlikely that material helpful to the defense will be recovered from this phone even if it is found to be reviewable.").[2] But there are many other reasons that material may be helpful to the defense. "Information that is not exculpatory or impeaching may still be relevant to

[2] It is unclear if the government is preemptively asserting here that the defense also may not inspect this thus-far unreviewed device if it is found to be reviewable. If so, the logic of this argument is flawed because the government has no basis to assume the contents of an unsearched iPhone based on evidence recovered from other, unrelated digital devices.

developing a possible defense. Even inculpatory evidence may be relevant." *United States v. Muniz-Jaquez*, 718 F.3d 1180, 1183 (9th Cir. 2013).

The government also contends that the defense's discovery request is overbroad because "it is difficult to conceive" how information on the digital devices from before the accident trip itself "could have any possible bearing on defendant's criminal misconduct aboard the *Conception*." (Gov't Opp. at 21:12-16). But the government's own Indictment bases Mr. Boylan's liability upon a much broader timeline ("Beginning on an *unknown date*, and continuing until on or about September 2, 2019") (emphasis added), and upon a much broader scope of conduct than solely his actions during this particular trip ("failure to conduct sufficient fire drills;" "failure to conduct sufficient crew training"). (Dkt. 1). Many of the case-specific facts establishing materiality for the remaining evidence contained on the devices has been submitted to the Court *in camera*. *See United States v. Hernandez-Meza*, 720 F.3d 760, 768-69 (9th Cir. 2013) ("A defendant needn't spell out his theory of the case in order to obtain discovery. Nor is the government entitled to know in advance specifically what the defense is going to be.").

At bottom, the government's narrow interpretation of what information is material to preparing the defense proves the point underlying the Motion — that the government is not knowledgeable about the defense's theories and case strategies, and need not be to comply with the defense's request for material under Rule 16. (*See* Mot. at 5 (*quoting Hernandez Meza*, 720 F.3d at 768).) It follows that the defense should not have to rely on the government's self-selection of materials from the digital devices.

This is particularly true because the government has not disclosed to the defense any search protocols or explanation of how the agent searched for and seized data from the devices. Under the mistaken belief that consent to search was required before accessing one of the devices, the government concedes that it constrained itself to the "limited consent" it received to search the device. Under the "limited consent," the agents only seized evidence "related to [the government's] investigation." (Gov't Opp.

at 9:10-19.) The government identifies no search protocols used by the agent to make this determination, and, as discussed above, the government takes a narrow view of the relevant timeframe and the agent is not privy to the theory of defense. While the government contends that the warrants had "extensive search protocols," (Gov't Opp. at 9, n. 5) at least one of the devices was not searched pursuant to a warrant but to what the government describes as a "limited consent." The warrants themselves provide that their "special procedures" govern only the searches of devices under the warrant and not to searches of any other devices, which would presumably include devices searched by consent. (Gov't Opp., Exh. 1, Attachment B at BOYLAN_00330910.) More importantly, the warrants themselves do not have "search protocols" but "search procedures." Those procedures required the search team to conduct the searches "only by using search protocols specifically chosen to identify only the specific items to be seized." (*Id*. at BOYLAN_00330908.) The government has not identified the search protocols — a list of search terms, keywords, or time periods, and so on — it used to search and seize data from the devices, even though the warrant, which the government was under the mistaken belief that it had to obtain and follow, required using such protocols in its "search procedures" section.[3] By choosing not to disclose any such protocol or methodology employed by the agent in determining how to conduct his search, the government's argument boils down to "just trust us."

As to the second category, the Motion articulated why the defense is entitled to inspect the devices from which the government intends to offer evidence at trial. This includes the need to evaluate the government's methods of repairing and forensically

---

[3] The government did produce in discovery the search protocol—a list of search terms and search term combinations—it used to search electronic devices seized from Truth Aquatics pursuant to a search warrant with a nearly identical "search procedures" section. The government also produced communications between the assigned AUSA and searching agents about how to modify these search terms given the time it would take to search the devices. No similar production has been made with respect to the decedents' digital devices.

examining the devices, determine how artifacts on the devices were used, and validate the limited files produced by the government, among others. Such an evaluation is crucial to Mr. Boylan's ability to assess the credibility of the government's witnesses who will testify about the digital evidence and to conduct an effective cross-examination of those witnesses. *See United States v. Cedano-Arellano*, 332 F.3d 568, 571 (9th Cir. 2003) (holding that it was erroneous for the district court to deny a defense motion for narcotics dog's certification and training records because the materials were necessary to defense counsel's ability to assess the dog's reliability and to conduct an effective cross-examination of the dog's handler). In addition, the suppression of evidence that goes to the reliability or credibility of those witnesses would violate the constitutional mandate of *Brady v. Maryland*, 373 U.S. 83 (1963).

The government responds, in part, that it has given the defense all the information needed to "challenge the technical aspects of the digital device searches" through the Cellebrite reports it has already produced in discovery. (Gov't Opp. at 22:16-19). This is simply incorrect. The government has produced limited reports through Cellebrite Reader, a tool used to share information selected by a reviewer. It does not contain the complete set of artifacts obtained through a forensic extraction, which can be recovered only through a physical examination. As an illustration of the limitations of the data that the government has produced, the defense attaches as Exhibit H a video that was produced and released by Cellebrite. The video is narrated by Heather Mahalik, the Senior Director of Digital Intelligence at Cellebrite and a renowned forensic expert. Ms. Mahalik explains the many limitations of Cellebrite Reader. (*See* Exh. H). For example, Cellebrite Reader cannot carve for additional artifacts that are unrecoverable without the extraction files and loading the subsequent extraction files into Cellebrite Physical Analyzer. Data carving through hex searching and verification of the information being presented is impossible. Cellebrite reports are designed as a collaboration tool to export and share information but are not a substitute for the government fulfilling its discovery obligations under Rule 16.

III. CONCLUSION

The defense is sensitive to the fact that digital devices contain personal information. For that reason, a protective order was proposed that would address how the devices are to be handled. This is not a matter of satisfying Mr. Boylan's curiosity, but of fulfilling the requirements of Rule 16 as the parties prepare to proceed to trial. Accordingly, all digital devices belonging to decedents should be disclosed to the defense to conduct its own independent examination.

Respectfully submitted,

CUAUHTEMOC ORTEGA
Federal Public Defender

DATED: April 10, 2023

By */s/ Georgina Wakefield*
GEORGINA WAKEFIELD
Deputy Federal Public Defender